Chapter 2: Perfect Secrecy, Product Cryptosystems

Math 495, Fall 2008

Hope College

September 15 and 17, 2008

A Second Example

- Suppose $\mathcal{P} = \{a, b, c, d\}$, $\mathcal{C} = \{A, B, C, D\}$, and $\mathcal{K} = \{K_1, K_2, K_3, K_4\}$ with encryptions as defined below:

	a	b	c	d
K_1	A	D	B	C
K_2	C	B	D	A
K_3	D	A	C	B
K_4	B	C	A	D

  Suppose that the probabilities on the plaintexts $\{a, b, c, d\}$ are $\{3/8, 1/4, 1/4, 1/8\}$, respectively, and that the key probabilities on $\{K_1, K_2, K_3, K_4\}$ are $\{1/4, 1/4, 1/4, 1/4\}$.
- Find $\Pr[y|x]$ for every $y \in \mathcal{C}$ and $x \in \mathcal{P}$. Does this cryptosystem exhibit perfect secrecy?

- **Theorem 2.3:** Suppose the 26 keys in the shift cipher are used with equal probability 1/26. Then for any plaintext probability distribution, the shift cipher has perfect secrecy.
- In order to prove this, we will compute $\Pr[y]$ and $\Pr[y|x]$ and show that they are equal.
- Then, from Bayes' Theorem, it follows that

$$\Pr[x|y] = \frac{\Pr[y|x]\Pr[x]}{\Pr[y]} = \Pr[x]$$

for all $x \in \mathcal{P}$ and $y \in \mathcal{C}$.

A Characterization of Perfect Secrecy

Theorem 2.4: A cryptosystem $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ with $|\mathcal{P}| = |\mathcal{C}| = |\mathcal{K}|$ provides perfect secrecy if and only if every key is used with equal probability $1/|\mathcal{K}|$, and, for every $x \in \mathcal{P}$ and $y \in \mathcal{C}$ there is a unique key such that

One-time Pad

A **one-time pad** is a cryptosystem based on an integer $n \geq 1$ with $\mathcal{P} = \mathcal{C} = \mathcal{K} = (\mathbb{Z}_2)^n$. For $x = (x_1, \ldots, x_n) \in \mathcal{P}$ and $(K_1, \ldots, K_n) \in \mathcal{K}$, we have

$$e_K(x) = (x_1, \ldots, x_n) + (K_1, \ldots, K_n) \pmod 2.$$

The decryption function is

$$e_K(y) = (y_1, \ldots, y_n) + (K_1, \ldots, K_n) \pmod 2.$$

Product Cryptosystems

Given two cryptosystems $\mathbf{S}_1 = (\mathcal{P}, \mathcal{P}, \mathcal{K}_1, \mathcal{E}_1, \mathcal{D}_1)$ and $\mathbf{S}_2 = (\mathcal{P}, \mathcal{P}, \mathcal{K}_2, \mathcal{E}_2, \mathcal{D}_2)$, the **product $\mathbf{S}_1 \times \mathbf{S}_2$** is defined as

$$(\mathcal{P}, \mathcal{P}, \mathcal{K}_1 \times \mathcal{K}_2, \mathcal{E}, \mathcal{D}).$$

Given $x \in \mathcal{P}$ and a key $K = (K_1, K_2)$, we encrypt via

$$e_K(x) = e_{K_2}(e_{K_1}(x)),$$

and decrypt by

$$d_K(y) = d_{K_1}(d_{K_2}(y)).$$